



SEGURIDAD INFORMATICA

Propuesta de investigación

DESCRIPCIÓN BREVE

En esta investigación se entenderá como seguridad informática, a la forma de protección frente ataques informáticos por parte de intrusos que tienen acceso no autorizado a dichas redes de trabajo. Y que tan confiable son los mecanismos de seguridad como los IDs que manejen las empresas.

Autores

Barrios Castillo Sayuris

Vargas Barreto José

INGENIERIA DE SISTEMAS

Noveno Semestre

UNIVERSIDAD DE CARTAGENA
CREAD Carmen de Bolívar

TABLA DE CONTENIDO

	Pág.
RESUMEN	2
INTRODUCCIÓN	3
I. MARCO GENERAL	4
1.1. PLANTEAMIENTO DEL PROBLEMA	4
1.2. DESCRIPCIÓN DEL PROBLEMA	6
1.2.1. Caracterización	6
1.2.2. Posibles Causas	6
1.2.3. Manifestaciones	7
1.2.4. Efectos Posibles	7
1.3. FORMULACIÓN DEL PROBLEMA	8
2. OBJETIVOS	9
2.1.OBJETIVO GENERAL	9
2.2.OBJETIVOS ESPECÍFICOS	9
3. JUSTIFICACIÓN	10
4. HIPOTESIS Y VARIABLE	11
5. ALCANCE Y LIMITES	12
II. MARCO TEORICO	13
2.1. ANTECEDENTES	13
2.2. MARCO CONCEPTAL	24
2.2.1. Marco Temático	24
2.2.2. Marco Tecnológico	34
2.2.3. Marco Legal	37
III. MARCO METODOLOGICO	42
3.1. TIPO DE INVESTIGACIÓN	42
3.2. POBLACIÓN Y MUESTRA	42
3.3. OPERACIONALIZACIÓN DE LAS VARIABLES	43
3.4. INSTRUMENTO DE INVESTIGACIÓN	44
3.5. RESULTADOS ESPERADOS	47
4. BIBLIOGRAFÍA	48

Resumen

Consideramos que la Seguridad Informática es una temática importante en nuestro campo como Ingenieros de Sistemas por ello nuestra Investigación se centra en su estudio. A lo largo de la investigación observaremos como en nuestro trabajo y vida cotidiana se maneja un flujo de información continuo, muchos de estos datos son confidenciales, por ende necesitan ser manejados con la mayor discreción por ello se implementan medidas de seguridad como password, anti virus, IDs... en las organizaciones, para prevenir ataques informáticos que puedan divulgar información confidencial o que piratas o hackers puedan detectar vulnerabilidades en el sistema.

Por ello en esta investigación centramos nuestro interés en este tema tan controversial, ya que en la actualidad se vienen presentando inconvenientes como el robo de información confidencial por parte de hackers y otro tipo de piratas informáticos, mostraremos como desde años atrás se viene presentando esta problemática y que medidas podemos tomar para evitar que siga sucediendo.

Para ello se estudiara una población en específico la cual será de ámbito empresarial, es decir; empresas que manejen alta cantidad de información confidencial en el Municipio de El Carmen de Bolívar; como los sectores financieros, de empresa y de gobierno; los cuales manejen bases de datos las cuales tienen acceso restringido.

Una vez hecha nuestra investigación previa y análisis de la información recolectada daremos inicio a nuestro trabajo de campo en el área del personal de la entidad donde pondremos en práctica lo trabajado en la unidad.

INTRODUCCIÓN

El desarrollo tecnológico ha tenido trascendentales cambios, el cual incorpora un alto volumen de información y los sistemas que la proveen; el aumento de las vulnerabilidades y las amplias amenazas, tales como las amenazas cibernéticas entre otros inconvenientes en cuestión de seguridad, los cuales no son conocidos por todos los usuarios de la red de trabajo.

En esta investigación se entenderá como seguridad informática, a la forma de protección frente ataques informáticos por parte de intrusos que tienen acceso no autorizado a dichas redes de trabajo. Y que tan confiable son los mecanismos de seguridad como los IDs que manejen las organizaciones.

La idea de este trabajo es que las personas aprendan a valorar lo importante que es la información, tanto para las grandes como pequeñas y medianas empresas y contar con sistemas de seguridad que alejen visitas de posibles hacker; y no solo las empresas tengan medidas de seguridad, también las personas que manejen redes sociales, E-mail, compras virtuales y todos los medios tecnológicos en los cuales manejen información confidencial o de suma importancia.

La necesidad de aumentar la seguridad informática de las operaciones críticas ha crecido marcadamente hace algunos años, como resultado del enorme aumento del uso de la tecnología de la información.

La presente propuesta tiene su origen en un problema concreto que es la forma en como es manejada la información dentro de una empresa y sus niveles de seguridad en las redes o en sistemas de información, el cual se ha enfrentado diariamente por el sector financiero, productivo, gobierno, instituciones, empresas y usuarios particulares; este es las vulnerabilidades de los sistemas de seguridad que permiten salvaguardar su información, o sea tener estrategias adecuadas para la seguridad cibernética; para lo que se ha realizado en esta propuesta las formas de ataques informáticos y cómo prevenirlos.

I. MARCO GENERAL

1.1 PLANTEAMIENTO DEL PROBLEMA

Teniendo en cuenta que desde el inicio de la humanidad hacer intercambio de información ha jugado un papel demasiado importante, porque es la manera eficaz de que la información que se maneje en dichos mensajes sea netamente confidencial.

Tanto en la milicia, diplomacia y el espionaje, constituyen la mejor defensa de las comunicaciones y datos que se transmiten, por cualquier canal. Esto es debido a la necesidad de que algunos de los mensajes solo sean conocidos por aquellas personas a las que van dirigidos y no puedan ser interpretados por nadie más que por ellos.

Concretando que nos encontramos en la era de la información como algunos llaman a la época en la que vivimos, ¿qué se puede pensar de la protección de la información? este es uno de los retos más fascinantes de la informática del futuro.

Representada por archivos confidenciales o mensajes que se intercambian dos o más interlocutores autenticados y cuyo contenido en muchos casos debe mantenerse en forma confidencial por razones personales, empresariales, políticas o de otra índole, la información es el bien máspreciado en estos días.

Es por estos motivos que la seguridad y confidencialidad de nuestra información abarca cada día una mayor importancia, ya que la tecnología va trayendo consigo nuevas alternativas de comunicación, no obstante, dentro de este mundo de comunicaciones existe la posibilidad de que nuestra información sea saqueada por otras personas.

Ya sea información personal o de tipo empresarial, siempre ha existido un porcentaje de inseguridad en el ámbito informático, existen métodos como los mensajes cifrados antiguamente llamados criptografía, contrarrestando esta situación; aunque se crea un gran interrogante ¿está realmente segura nuestra información?, existiendo en la actualidad los llamados hackers, piratas informáticos, entre otros, que navegan en la web buscando puntos vulnerables solo para obtener información totalmente confidencial mediante ataques informáticos.

Como ven es un problema complejo, ya que así como pueden atacar a empresas aun cuando constan con IDs, pueden acceder a cuentas personales, redes sociales; esta

problemática ha llegado hasta el punto de que están clonando las tarjetas bancarias y para contrarrestarlo los bancos recomiendan a los usuarios usar tarjetas con chip.

Es allí donde nace la necesidad de saber que tan efectivos son estos métodos de seguridad, y que tan seguras se sienten las personas con los métodos de seguridad informática o tecnológicas en la actualidad.

1.2 DESCRIPCION DEL PROBLEMA

1.2.1. Caracterización:

Esta problemática se presenta más que todo en las personas que manejan redes sociales, E-mail, entre otras cuentas o aplicaciones en sus teléfonos móviles, en las cuales tienen acceso a juegos o encuestas; en donde manejan un alto grado de información.

Por otro lado, también se presenta en el entorno laboral, en empresas que manejan bases de datos o información confidencial. Hospitales, centros de acreditación, empresas telefónicas, EPS, inclusive en los bancos.

Esta investigación va dirigida a la población empresarial del Carmen de Bolívar, Bolívar para comprobar que tan optima esta la seguridad informática en esta zona.

1.2.2 Posibles Causas:

La principal causa que da inicio a la seguridad informática surge de la necesidad de proteger la información confidencial; en la antigüedad los ejércitos utilizaban la criptografía con el fin de que el enemigo no pudiera saber cuáles eran sus verdaderos planes, de esta manera lograron muchas veces mantener sus objetivos en total discreción.

La criptografía desde los tiempos de la Grecia Clásica en la Cultura Occidental por ejemplo, ha sido un componente esencial de la seguridad en las comunicaciones. Si bien hasta mediados del siglo XX era del dominio casi exclusivo de sectores gubernamentales (militares y diplomáticos) o de grandes corporaciones (la Iglesia Católica por ejemplo) en la actualidad se utiliza por toda la sociedad, en cualquier comunicación digital.

Estos métodos de seguridad nacen por la necesidad de evitar los delitos informáticos, y filtraciones de información confidencial entre otros.

1.2.3 Manifestaciones:

Por poner sólo un ejemplo sencillo y común, un gran problema en la actualidad es el asociado con el correo electrónico que se transmite a través de redes y cuyo nivel seguridad deja mucho que desear.

Internet es un claro ejemplo de estas amenazas, en tanto es un entorno abierto en su sentido más amplio. Por lo visto en estos pocos años de existencia de la llamada red de redes, sobran los comentarios acerca de pérdida de privacidad, accesos no autorizados, ataques y otros delitos informáticos a nivel nacional e internacional.

Muchos usuarios han perdido información de tipo personal y empresarial mediante correos electrónicos, o peor aún mediante las redes sociales han intercambiado información que ha sido jaqueada por terceros, en el peor de los casos cuentas desbancadas porque han accedido a sus claves ya sea que hayan clonado sus tarjetas débito o crédito; por eso hoy en día los bancos u otras empresas han optado por implementar tarjetas con chip, buscando la manera eficaz de proteger el patrimonio de los clientes.

1.2.4 Efectos Posibles:

- Pérdida de información confidencial e importante.
- Estafas
- Robo en cuentas bancarias haciendo que el cliente pierda su único patrimonio económico.
- Impedimento de la ejecución a planes por causa de infiltración Ej. Las llamadas chuzadas del DAS, fallas en planes policiales, fallas en operativos del ejército.
- Amenazas a funcionarios públicos. Entre muchas otras.

1.3 FORMULACION DEL PROBLEMA

¿Existe confiabilidad en los sistemas informáticos?

- **¿Se toman medidas de prevención en las empresas que manejan una alta cantidad de información?**
- **¿Qué tan optimo es el nivel de seguridad de las empresas?**

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Conocer si existe confiabilidad en los sistemas informáticos

2.2 OBJETIVOS ESPECIFICOS

- Conocer si se toman medidas de prevención en las empresas que manejan una alta cantidad de información
- Conocer que tan optima es la seguridad de las empresas

3. JUSTIFICACIÓN

¿Por qué y para que seleccionamos el tema?

El motivo por el cual seleccionamos ese tema es porque la informática siempre nos ha llamado la atención y porque los delitos informáticos están estrechamente relacionados con la informática de este modo debemos tener nociones de cómo combatirlos para compartir o guardar de forma segura nuestra información.

CAUSAS Y PROPÓSITOS.

Una de las causas que anteriormente les mencionamos es por satisfacción propia, pero también porque los delitos informáticos son una nueva forma de criminalidad que están ocasionando graves problemas y se necesita buscar soluciones ya que hoy en día no hay suficientes formas de combatirlos. El propósito de nuestra investigación es analizar el concepto de delito informático así como sus diferentes tipos, estadística, seguridad, legislación de estos, y muchas otras cosas importantes relacionadas con el crimen informático.

Una parte importante de la sociedad desconoce este tipo de términos, algunos ni siquiera le dan la importancia necesaria, ya que desconocen los alcances que pueden llegar a tener cada uno de ellos. Aparentemente los ciberdelitos y el ciberterrorismo, físicamente no lastiman a las personas ni causan daños importantes, razón por la cual, esta investigación se ha basado en antecedentes que hoy en día se pueden proyectar para generar posibles escenarios como resultado de un ataque. Hay que recordar que el ser humano se caracteriza por aprender de sus errores, para que sus resultados se asemejen lo más posible a la perfección, y el caso de este tipo de personas no es la excepción, su reputación depende del éxito de cada una de sus acciones u operaciones.

4. HIPÓTESIS Y VARIABLE

La principal característica de los delitos informáticos es que la mayoría aún no están contemplados dentro de las leyes de muchos países y por lo tanto no son sancionados.

El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Por su mal manejo ha abierto la puerta a conductas antisociales y delictivas.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

VARIABLES INDEPENDIENTES:

- La débil estructura de nuestro país para defenderse de los delitos informáticos.
- La inseguridad en las páginas de Internet donde se realiza el comercio informático y la falta de educación informática.
- El actual crecimiento del fenómeno de los “Hackers”.

VARIABLES DEPENDIENTES:

- Inseguridad en las redes.
- Debilitación del comercio electrónico.

5. ALCANCE Y LIMITES

Esta investigación está centrada en las empresas del sector financiero en el Municipio de El Carmen de Bolívar, de este modo se contará con un diseñado plan de trabajo para poder cubrir todo este sector.

Teniendo en cuenta que este es un amplio sector limitaremos nuestra investigación a una sola empresa de este sector, ya que se cuenta con diversas empresas y dentro del plan de trabajo nos debemos centrar en nuestros objetivos específicos, sin dejar de lado nuestro objetivo general que incluye a todo el sector empresarial de este Municipio.

II. MARCO TEORICO

2.1 ANTECEDENTES

Nº	TITULO	AUTORES	TIPO DE DOCUMENTO	DIRECCIÓN ELECTRONIA
1	Propuesta de Seguridad	Fernando Bugarini Hernández	Tesis	http://tesis.ipn.mx/bitstream/handle/123456789/498/TESIS%20PROPUESTA%20SEGURIDAD.pdf?sequence=1
2	Delitos Informáticos	José Alberto Cruzado Reyes	Propuesta de Investigación	https://beorlegui.files.wordpress.com/2011/10/delitos-informaticos-y-ciberterrorismo.pdf
3	Seguridad Informática Sus Implicancias e Implementación	Cristian Fabián Borghello	Tesis	https://www.seguinfo.com.ar/tesis/
4	Seguridad de la Información	Secretaria de Economía	Documento	http://www.firmadigital.gob.mx/Seguridad.pdf
5	Seguridad en Redes y Datos	Luis Orellana Rafael Hernández	Tesis	http://rd.udb.edu.sv:8080/jspui/bitstream/123456789/265/1/033380_tesis.pdf
6	Auditoria De Seguridad De Redes Inalámbricas De Área Local Wireless Local Area Network (Wlan)	Claudia Monzón Michel	Tesis	http://bibliotecadigital.umsa.bo:8080/rddu/bitstream/123456789/1256/1/314_T-1854.pdf
7	“Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial”	María Gabriela Hernández Pinto	Tesis	https://www.dspace.espol.edu.ec/bitstream/123456789/10730/7/TESIS%20Mar%C3%ADA%20Gabriela%20Hern%C3%A1ndez%20Pinto.pdf

TESIS: PROPUESTA DE SEGURIDAD DEL INSTITUTO POLITÉCNICO NACIONAL.

La informática esta hoy día presente en todos los campos de la vida cotidiana, el ser humano enfrenta varios procesos tecnológicos y comienza a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente.

El progreso cada día es más importante y pone a disposición de la sociedad una cantidad de información de toda naturaleza, al alcance de millones de interesados y de usuarios. Las más diversas esfera del conocimientos humano en los científico en lo técnico, y en lo profesional están siendo incorporados en sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo dese, en un conjunto de datos que hasta hace unos años solo podría ubicarse luego de largas búsquedas y selecciones, en que el hombre jugaba un papel determinate y las maquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, este enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar a el receptor mediante sistemas sencillos de operar confiables y capaces de responder a casi toda la gama de interrogantes que se planten a los archivos informáticos.

Este es el panorama del nuevo fenómeno científico-tecnológico en las sociedades modernas. Por eso ha llegado a sostenerse que la informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de los gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y posibilidades de juegos lícitos e ilícitos en donde es necesario el derecho para regular múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Los progresos mundiales de las computadoras, el reciente aumento de las capacidades de almacenamiento y procesamiento, la miniaturización de los chips las computadoras instalados en productos industriales, la fusión de procesos de la información con la nuevas tecnologías de la información, así como la investigación en el campo de la inteligencia artificial. Ejemplifican el desarrollo actual definido a menudo como la “era de la información”. Pero así como la informática ha venido a transformar

gran parte de la información, lo que ha ocasionado un gran avance en todos los aspectos, también tiene algunas situaciones que son indispensables tomar en cuenta como la seguridad para los archivos, bases de datos que los usuarios de la misma elaboran y que en el caso de las empresas es sumamente importante resguardar por razones obvias.

En la última década, en todo el mundo la seguridad cibernética ha comenzado a cobrar relevancia, en Colombia el mundo digital se ha integrado en toda la sociedad de una forma vertiginosa, en nuestro diario vivir son más las personas que se apoyan en Internet para utilizar sus servicios y realizar sus actividades, enviar un correo electrónico, participar en un foro de discusión, tener una sesión de chat, comunicación de voz sobre IP, descargar música o el libro favorito, hacer publicidad, etc.

Son algunas de las cosas más comunes. Sin embargo, el mundo de los negocios empresariales es aún más complejo y la gama de servicios nos presenta mayores alternativas. Las “transacciones” electrónicas nos permiten ahorrar tiempo y recursos, pagar los servicios públicos, transferir de una cuenta bancaria a otra, participar en una subasta para comprar un vehículo, pagar un boleto de avión etc. En todos estos ejemplos hay algo en común, el dinero, y cuando hablamos de tan escaso pero tan apreciado bien las empresas deben garantizar la implementación de políticas de seguridad informática.

Los que trabajan en el mundo empresarial, deben recibir instrucciones claras y definitivas que los ayuden a garantizar la seguridad de la información en el complejo mundo de los negocios. Cada vez encontramos más gerentes interesados en entender las reglas del negocio, entre ellas las referentes a las políticas de seguridad informática. El ofrecer productos o servicios a través de Internet sin tomar en cuenta la seguridad informática no sólo denota negligencia, sino que constituye una invitación para que ocurran incidentes de seguridad que podrían dañar severamente la reputación y afectar los ciclos del negocio.

El secreto del éxito, tanto individual como de un negocio, de una empresa estatal, etc., depende cada vez más de la habilidad para poder comunicarse con cualquiera, en tiempo real y con los niveles de seguridad necesarios. La aparición de la conectividad generalizada a través de Internet, así como de dispositivos cada vez más potentes y

omnipresentes, ha causado una revolución en el terreno de las comunicaciones y la informática.

Con los beneficios que nos brindan las nuevas posibilidades de conectividad, emergen también una serie de nuevos riesgos. Muchas empresas son amenazadas en sus activos, y más aún cuando el activo más importante es la información.

El deterioro de ésta puede representar millones de dólares en pérdidas en el mundo de los negocios. Las vulnerabilidades en los sistemas de información pueden traer graves problemas. Cada vez las redes están expuestas a virus informáticos, spam, código malicioso, hackers y crackers que penetran los sistemas de seguridad. Los elementos que la seguridad de la información busca protegerla información, los equipos que la soportan, las personas que la utilizan.

Es importante tener claro cuáles son los tipos de amenazas más comunes a las cuales están expuestas las empresas hoy en día.

El análisis y evaluación de riesgos permite a las compañías tener una visión más clara sobre sus vulnerabilidades y de los esfuerzos que deben hacer para mejorar.

Tipos de Amenazas	Ejemplo
Suplantación	• Falsificar mensajes de correo electrónico • Reproducir paquetes de autenticación
Alteración	• Alterar datos durante la transmisión • Cambiar datos en archivos
Repudio	• Eliminar un archivo esencial y denegar este hecho • Adquirir un producto y negar posteriormente que se ha adquirido
Divulgación de información	• Exponer la información en mensajes de error • Exponer el código de los sitios Web
Denegación de servicio	• Inundar una red con paquetes de sincronización • Inundar una red con paquetes ICMP falsificados
	• Explotar la saturación de un búfer para

Elevación de privilegios	obtener privilegios en el sistema • Obtener privilegios de administrador de forma ilegítima
--------------------------	--

DELITOS INFORMATICOS:

Hoy en día las comunicaciones se hacen más accesibles cada vez más a todo el mundo, razón por la cual (entre otras muchos otros factores más) estamos a la merced de los delitos en la red. Los riesgos que conlleva el ser víctima de alguno de ellos pueden ser desde algo mínimo hasta algo muy considerado como la afectación a infraestructuras gubernamentales o privadas. Es necesario, para las personas que conocemos este mundo de la computación, preocuparnos por los sistemas de seguridad para los usuarios y buscar diferentes estrategias para la protección contra este tipo de acciones sancionadas por el derecho penal.

¿QUÉ ES UN DELITO INFORMATICO?

Se considera un “Delito informático” o “Crimen Electrónico” a aquella acción conducta ilícita susceptible a ser sancionada por la ley, por medio del uso correcto de internet, que tiene como objetivo esencial el destruir y dañar computadoras, medios electrónicos y redes de internet. Los delitos informáticos, al igual que la tecnología evoluciona y se hace más complejo al pasar de los días, razón por la cual el termino anterior se puede ampliar a la inclusión de delitos como el fraude, el robo, el chantaje, violación a los derechos de autor, pornografía infantil, sabotaje, la falsificación y principalmente la manipulación de transferencias bancarias. Con el desarrollo de la programación y el internet, los delitos informáticos se han vuelto más frecuentes y sofisticados, y con ello la seguridad completa no existe, dado que cuando se llega a presentar alguna situación de esta naturaleza, el usuario configura un sistema de seguridad para la amenaza presentada, pero al poco tiempo deja de ser funcional ya que el móvil del ciberdelincuente cambia, y con ello la probabilidad de una fuga importante de información del usuario.

CLASIFICACIÓN

Dentro de las acciones legales en contra de esta nueva versión de delincuencia, se pueden dividir estas categorías de crímenes en dos grupos:

1. Como fin u objetivo.- Crímenes que tienen como objetivo redes de computadoras, por ejemplo, con la instalación de códigos, gusanos y archivos maliciosos, spam, ataque masivos a servidores de Internet y generación de virus.

2. Como instrumento o medio.- Crímenes realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, pornografía infantil, pedofilia, etc.

SUJETOS ACTIVOS Y PASIVOS

Así como en la vida real, se les otorga una clasificación a los criminales por la forma de ejecución de sus crímenes, como por ejemplo, psicópatas, asesinos en serie etc., en el ciberespacio también sucede lo mismo, por las características específicas tales como la habilidad para el manejo de los sistemas o la realización de tareas que le facilitan el acceso a información sensible. En algunos casos la motivación del delito no es económica, sino simplemente el deseo de hacer conocer a otras personas o simplemente ejercitar sus conocimientos.

ACTIVOS

Son aquellos que poseen ciertas características que no presentan el denominador común en los delincuentes, generalmente los activos se encuentran en un campo laboral específico, ya sea que estén involucrados en el manejo de información sensible, o bien poseen la habilidad de manejo de los sistemas informáticos. Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland. Esta categoría requiere que:

1. El sujeto activo del delito sea una persona de cierto estatus socioeconómico
2. Su comisión no pueda explicarse por falta de medios económicos, carencia de recreación poca educación, poca inteligencia, ni por inestabilidad emocional

PASIVOS

A diferencia del activo, el pasivo que se le dará el nombre de "víctima del delito", es aquella sobre la cual recaen las acciones en general que realiza el activo. Mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Pueden ser individuos que laboren en instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

ANTECEDENTES INTERNACIONALES

“El ciberespacio no es lo mismo que el espacio exterior, y podemos seguir la pista y detener a cualquiera” Sin duda alguna, uno de los antecedentes a renombrar en esta investigación, es el caso de Vladimir Levin quien en un principio de su vida profesional se dedicó al estudio de la ciencia, decidió abandonarla para comenzar a enfocarse en los sistemas informáticos de entidades financieras. Perteneciente a el equipo de trabajo AO Saturn en San Petersburgo, Vladimir comienza con los que fueran sus primeros crimines virtuales. Desde que, accedió a la red del Citibank en donde obtuvo un listado de códigos de cuentas y contraseñas 7 de los diferentes usuarios. Durante las primeras semanas logro transferir alrededor de 3.7 millones de dólares a diferentes cuentas ubicadas en los países de Argentina, Estados Unidos, Finlandia, Holanda, Alemania e Israel. Cuando el banco notó las transferencias contactaron con las autoridades, quienes siguieron la pista durante meses hasta Levin, quien finalmente sería arrestado por la INTERPOL en 1995 en el aeropuerto de Heathrow, en Inglaterra y más tarde extraditado a los Estados Unidos.

IMPACT

La Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) es una que colaboran en la mejora de la capacidad de la comunidad mundial para evitar los ataques, defenderse de ellos y ofrecer la respuesta adecuada La colaboración entre la UIT (Unión Internacional de Telecomunicaciones) e IMPACT ofrece a los 191 Estados Miembros de la UIT los recursos y conocimientos técnicos especializados para fomentar la ciberseguridad en sus propios países y fuera de ellos. Alianza de gobiernos, dirigentes de la industria y expertos en ciberseguridad.

TESIS: SEGURIDAD INFORMÁTICA SU IMPLICANCIA E IMPLEMENTACIÓN –
CRISTIAN F. BORGHELLO AÑO 2001.

ANÁLISIS DEL OBJETIVO DE LA SEGURIDAD INFORMÁTICA

Para comenzar el análisis de la Seguridad Informática se deberá conocer las características de lo que se pretende proteger: la Información Así, definimos **Dato** como “la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa “lo que se da”. La Información “es una agregación de datos que tiene un significado específico más allá de cada uno de éstos”, y tendrá un sentido particular según cómo y quién la procese.

Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información. Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser pública: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que debe ser privada: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.
2. Es Valiosa: es un activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorías. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se “filtran” a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades. Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- Protección a la Réplica: mediante la cual se asegura que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
- No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- Consistencia: se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- Aislamiento: este aspecto, íntimamente relacionado con la Confidencialidad, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.

- Auditoria: es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuándo las realiza. Cabe definir Amenaza, en el entorno informático, como cualquier elemento que comprometa al sistema.

ELEMENTOS DE LA SEGURIDAD INFORMÁTICA:

Integridad: Los componentes del sistema permanecen inalterados a menos que sean modificados por los usuarios autorizados.

Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Privacidad: Los componentes del sistema son accesibles sólo por los usuarios autorizados.

Control: Solo los usuarios autorizados deciden cuando y como permitir el acceso a la información.

Autenticidad: Definir que la información requerida es válida y utilizable en tiempo, forma y distribución.

No Repudio: Evita que cualquier entidad que envió o recibió información alegue, que no lo hizo.

Auditoria: Determinar qué, cuándo, cómo y quién realiza acciones sobre el sistema.

DELITO INFORMÁTICO:

Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. Se realizan por medios informáticos y tienen como objeto a la información en sí misma.

TIPOS DE DELITOS:

- Fraudes cometidos mediante manipulación de computadoras
- Manipulación de datos de E/S
- Daños a programas o datos almacenados
- Distribución de virus
- Espionaje
- Acceso no autorizado
- Reproducción y distribución de programas protegido por la ley

AMENAZAS HUMANAS:

- Hacker: persona curiosa, inconformista y paciente que busca su superación continua aprovechando las posibilidades que le brindan los sistemas.
- Cracker: hacker dañino.
- Phreaker: persona que engaña a las compañías telefónicas para su beneficio propio.
- Pirata Informático: persona que vende software protegido por las leyes de Copyright.
- Creador de virus Diseminadores de virus
- Insider: personal interno de una organización que amenaza de cualquier forma al sistema de la misma.

2.2. MARCO CONCEPTUAL

2.2.1. Marco Temático

Dentro de la investigación existen una serie de conceptos importantes, de los cuales debemos saber su importancia dentro de dicha investigación y a que se refieren entre los más destacados tenemos:

SEGURIDAD INFORMÁTICA

La seguridad informática, de igual forma a como sucede con la seguridad aplicada a otros entornos, trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada. Esta visión de la seguridad informática implica la necesidad de gestión, fundamentalmente gestión del riesgo. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de estos análisis, implantar medidas preventivas y correctivas que eliminen los riesgos asociados o que los reduzcan hasta niveles manejables.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software. A través de la adopción de las medidas adecuadas, la seguridad informática ayuda a la organización cumplir sus objetivos, protegiendo sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales.

INFORMACIÓN

La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Por lo tanto, otra perspectiva nos indica que la información es un recurso que otorga significado o sentido a la realidad, ya que mediante códigos y conjuntos de datos, da origen a los modelos de pensamiento humano.

DATOS

Son una representación simbólica (numérica, alfabética, algorítmica, entre otros.), un atributo o característica de una entidad. Los datos describen sucesos y entidades.

Los datos aisladamente pueden no contener información humanamente relevante. Sólo cuando un conjunto de datos se examina conjuntamente a la luz de un enfoque, hipótesis o teoría se puede apreciar la información contenida en dichos datos.

Los datos pueden consistir en números, estadísticas o proposiciones descriptivas. Los datos convenientemente agrupados, estructurados e interpretados se consideran que son la base de la información humanamente relevante que se pueden utilizar en la toma de decisiones, la reducción de la incertidumbre o la realización de cálculos.

Es de empleo muy común en el ámbito informático y, en general, prácticamente en cualquier disciplina científica.

IDS

(Sistema de detección de intrusos) Es un sistema que detecta manipulaciones no deseadas en el sistema, especialmente a través de internet. Las manipulaciones pueden ser ataques de hackers malintencionados.

MENSAJES CIFRADOS O CRIPTOGRAFÍA

Es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Su utilización es tan antigua como la escritura. Los romanos usaban códigos para ocultar sus proyectos de guerra de aquellos que no debían conocerlos, con el fin de que sólo las personas que conocían el significado de estos códigos descifren el mensaje oculto.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso.

ANTIVIRUS

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

ATAQUES INFORMÁTICOS

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.

Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques.

VULNERABILIDAD

En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Las vulnerabilidades son el resultado de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro.

MALWARE O CÓDIGOS MALICIOSOS

Constituyen también una de las principales amenazas de seguridad para cualquier Institución u Organizaciones y aunque parezca un tema trivial, suele ser motivo de importantes pérdidas económicas.

Esta amenaza se refiere a programas que causan algún tipo de daño o anomalía en el sistema informático. Dentro de esta categoría se incluyen los programas troyanos, gusanos, virus informáticos, backdoors, rootkits, entre otros.

TROYANOS

Es un software malicioso que permite la administración remota de una computadora de forma oculta y sin el consentimiento del propietario. Generalmente están disfrazados como algo atractivo o inocuo que invitan al usuario a ejecutarlo.

Pueden tener un efecto inmediato y tener consecuencias como el borrado de archivos del usuario e instalar más programas maliciosos. Son usados para empezar la propagación de un gusano, inyectándolo de forma local dentro del usuario.

GUSANOS

Los gusanos son programas que se transmiten a sí mismos, explotando vulnerabilidades en una red de computadoras para infectar otros equipos. Su principal objetivo, es infectar a la mayor cantidad posible de usuarios y también puede contener instrucciones dañinas al igual que los virus.

A diferencia de los gusanos, un virus necesita la intervención del usuario para propagarse, mientras que los gusanos se propagan automáticamente.

VIRUS INFORMÁTICO

Éstos, son los tipos más conocidos de software maligno que existen y se distinguen por la manera en que se propagan.

El término de virus informático se usa para designar un programa que al ejecutarse se propaga infectando otro software ejecutable de la misma computadora.

BACKDOORS

Es un método para eludir los procedimientos habituales de autenticación al conectarse en una computadora. Una vez que el sistema ha sido comprometido, puede instalarse una puerta trasera para permitir un acceso remoto más fácil en el futuro de los atacantes. Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, permaneciendo ocultos ante posibles inspecciones, utilizando troyanos, gusanos u otros métodos.

ROOTKITS

Es un software que modifica el sistema operativo de la computadora, para permitir que el malware permanezca oculto al usuario, evitando que el proceso malicioso sea visible en el sistema.

DELITOS INFORMATICOS

Con el término delito informático aglutinamos los hechos que, basándose en técnicas o mecanismos informáticos, pudieren ser tipificados como delito en el Código Penal, tales como: delito de estafa, delito contra la propiedad intelectual e industrial, etc. Debido a los avances tecnológicos y a los nuevos mecanismos para delinquir se ha hecho necesario introducir y modificar determinados artículos que permitan aglutinar éstos.

Partiendo de la base que no hay ningún apartado específico de delitos informáticos en el Código Penal, atenderemos a la clasificación de los mismos, siempre y cuando, los datos o sistemas informáticos formen parte de la comisión del delito, a saber:

- Las amenazas.
- Los delitos de exhibicionismo y provocación sexual.
- Los delitos relativos a la prostitución y corrupción de menores.
- Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio: El descubrimiento y revelación de secretos. La interceptación de correo vendría asimilada a la violación de correspondencia, siempre que no exista consentimiento y haya intención de desvelar secretos o vulnerar la intimidad de un tercero. También sería un delito contra la intimidad la usurpación y cesión de datos reservados de carácter personal.
- Delitos contra el honor: Calumnias e injurias, habiéndose especial mención cuando estas se realizaren con publicidad -se propaguen-.
- Las estafas. Entre muchos otros.

SOFTWARE ESPÍA (Spyware)

Spyware son programas espiones que constantemente monitorean los pasos del usuario de un computador conectado a la red de internet, sin su consentimiento, a fin de trazar un perfil comercial completo, tal el caso de proveedores de productos de tiendas virtuales, las que intentan captar informaciones que tengan utilidad para el

agente. Los programas tienen la capacidad de apoderarse de informaciones personales del usuario, que son transferidas digitalmente para la sede de una empresa o persona a fin de ser comercializadas.

E-MAIL

También llamado correo electrónico. Es un servicio de red para permitir a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos.

SPAM

Es cualquier mensaje enviado a varios destinatarios que no solicitaron específicamente tal mensaje. Por eso es conocido el spam como el correo electrónico basura.

Las personas que envían spam generalmente compran o generan una lista de direcciones de e-mail a los cuales les envían los mensajes. El origen de estos mensajes tiende a ser "falsificados," para ocultar quién realmente las envió.

CIBERESPACIO

Es un conjunto o realidad virtual donde se agrupan usuarios, páginas web, chats, y demás servicios de Internet y otras redes.

Internet constituye el mayor ámbito del ciberespacio. Aquí se incluyen la World Wide Web (Web), los grupos de noticias USENET y el Internet Relay Chat (IRC). A cualquiera de ellos es posible acceder con un acceso inalámbrico a Internet o con cualquier tipo de red que se tenga a la mano.

Aunque el ciberespacio no debe confundirse con el Internet real, el término se refiere a menudo a los objetos e identidades que existen dentro de la misma red informática, así que se podría decir, metafóricamente, que una página web "se encuentra en el ciberespacio". Según esta interpretación, los acontecimientos que tienen lugar en

Internet no están ocurriendo en los países donde los participantes o los servidores se encuentran físicamente, sino "en el ciberespacio".

REDES SOCIALES

son servicios prestados a través de Internet que permiten a los usuarios generar un perfil desde el que hacer públicos datos e interactuar con otros usuarios y localizarlos en la red en función de las características publicadas en sus perfiles.

Entonces, las redes sociales son estructuras sociales compuestas de grupos de personas, las cuales están conectadas por uno o varios tipos de relaciones, tales como amistad, parentesco, intereses comunes o que comparten conocimientos. En su forma más simple, una red social es un mapa de todos los lazos relevantes entre todos los nodos estudiados.

Otra opción es identificar la red que envuelve a una persona (en los diferentes contextos sociales en los que interactúa).

APLICACIONES

Programa informático que permite a un usuario utilizar una computadora con un fin específico. Las aplicaciones son parte del software de una computadora, y suelen ejecutarse sobre el sistema operativo.

Una aplicación de software suele tener un único objetivo: navegar en la web, revisar correo, explorar el disco duro, editar textos, jugar (un juego es un tipo de aplicación), etc. Una aplicación que posee múltiples programas se considera un paquete.

Son ejemplos de aplicaciones Internet Explorer, Outlook, Word, Excel, WinAmp, etc.

Una aplicación (también llamada app) es simplemente un programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático. Cabe destacar que aunque todas las aplicaciones son programas, no todos los programas son aplicaciones. Existe multitud de software en el mercado, pero sólo se denomina así a aquel que ha sido creado con un fin determinado, para realizar tareas concretas. No se consideraría una aplicación, por ejemplo, un sistema operativo, ni una suite, pues su propósito es general.

Las aplicaciones nacen de alguna necesidad concreta de los usuarios, y se usan para facilitar o permitir la ejecución de ciertas tareas en las que un analista o un programador han detectado una cierta necesidad. Pero las aplicaciones también pueden responder a necesidades lúdicas, además de laborales (todos los juegos, por ejemplo, son considerados aplicaciones). Se suele decir que para cada problema hay una solución, y en informática, para cada problema hay una aplicación.

TRANSACCIONES ELECTRÓNICAS

Debemos señalar que una transacción electrónica no es más que un contrato celebrado mediante medios electrónicos, a través de la red. En nuestra legislación el contrato, sea este de cualquier naturaleza, es el acuerdo de voluntades destinadas a crear, regular, modificar, o extinguir una relación jurídica patrimonial, entendida esta última como el vínculo legal de contenido económico que va surgir entre los contratantes.

RED

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.

También hay mensajes, que es lo que estos roles intercambian. La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más extendido de todo el modelo TCP/IP, basado en el modelo de referencia o teórico OSI.

IP

(Internet Protocol) Es la norma de comunicación que define como funciona internet. El protocolo IP se encarga del establecimiento de la comunicación entre dos dispositivos en una red.

WEB

Una web es aquella que consiste en un documento electrónico que contiene información, cuyo formato se adapta para estar insertado en la World Wide Web, de manera que los usuarios a nivel mundial puedan entrar a la misma por medio del uso de un navegador, visualizándola con un dispositivo móvil como un Smartphone o un monitor de computadora.

El formato de esta información puede ser XHTML o HTML y desde una web se puede entrar a otra con enlaces de hipertexto. Los recursos para la presentación de la información de una web pueden ser scripts, imágenes digitales, hojas en forma de cascada, entre otros. Para que una web pueda estar en línea y ser vista por cualquier persona, requiere de un hospedaje, cosa que puede hacerse en un servidor remoto o local. La composición de una página web consiste básicamente en información que puede presentarse con módulos multimedia y texto, lo cual se complementa con hiperenlaces para conducir a otras secciones de dicha web o a otras webs.

PIRATA INFORMÁTICO

Es aquél que hace uso de los recursos libres y / o de pago que pueden ser movidos a través de las vías de la información que conforman internet, telnet, entre otras; para beneficio propio y lucrativo. Por extensión, se considera pirata informático a quien hace uso de software que no ha adquirido en forma legal o a los costos formales.

HACKER

Es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc.

El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

CRACKER

Es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo. También se denomina cracker a quien diseña o programa cracs informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

INSIDER

En el contexto de la Seguridad de la Información, llamamos Insider a la persona perteneciente a la propia organización que provoca fugas de información (normalmente con su consentimiento). Estas personas suelen tener acceso a información sensible de la organización bien porque no contamos con las políticas de seguridad adecuadas o bien porque la propia organización le da acceso -consciente o inconscientemente- a esta información.

Un claro ejemplo de un Insider es el ejecutivo que se lleva la cartera de clientes cuando causa baja de la organización. No necesitan ser grandes expertos en informática, sólo tener el conocimiento y el criterio para distinguir esa información.

¿Cómo podemos identificarlos?

Identificar a un Insider no es tarea fácil, pero hay ciertas pautas de comportamiento que nos deben hacer sospechar que una persona de nuestra organización es un Insider.

Personas con alto conocimiento en ordenadores que los utilizan constantemente sin explicar qué hacen y acaparan esas tareas informáticas durante espacios prolongados de tiempo.

Empleados que trabajan hasta tarde sin razón, siempre con el ordenador sin explicar lo que están haciendo. Prefieren turnos con poca gente, incluso días festivos.

Empleados cuya labor poco tiene que ver con los ordenadores y los utilizan en la oficina.

2.2.2. Marco Tecnológico

IDs

Un sistema de detección de intrusos, es usado para detectar tráfico de red y uso de computadora maliciosos, que no pueden ser detectados por un cortafuego convencional.

Uno de estos sistemas está compuesto por múltiples componentes como: sensores que generan eventos de seguridad, una consola para monitorear eventos y alertar y controlar los sensores y un motor central que guarda los eventos en una base de datos y usa un sistema de reglas para generar alertas de seguridad.

ANTIVIRUS

Los antivirus son aplicaciones de software que han sido diseñados como medida de protección y seguridad para resguardar los datos y el funcionamiento de sistemas informáticos caseros y empresariales de aquellas otras aplicaciones conocidas comúnmente como virus o malware que tienen el fin de alterar, perturbar o destruir el correcto desempeño de las computadoras.

VIRUS

Los virus, gusanos, troyanos, spyware son tipos de programas informáticos que suelen ejecutarse sin el consentimiento (e incluso, conocimiento) del usuario o propietario de un ordenador y que cumplen diversas funciones dañinas para el sistema. Entre ellas, robo y pérdida de información, alteración del funcionamiento, interrupción del sistema y propagación hacia otras computadoras.

ATAQUES INFORMÁTICOS

Constan de cinco fases:

Fase 1: Reconocimiento. Esta etapa involucra la obtención de información con respecto a una potencial víctima que puede ser una persona u organización.

Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo.

En esta fase también pueden obtener información mediante llamadas telefónicas o

inclusive conversaciones directamente con empleados de la empresa atacada o persona a la cual se le hace el seguimiento.

Fase 2: Exploración. En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros.

Se realiza un tipo de conexión ya sea desde la máquina del atacante, o alguna maquina comprometida, de forma general se usan herramientas automáticas como un scanner de red, host, marcadores masivos, etc.

Fase 3: Obtener acceso. En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema descubiertos durante las fases de reconocimiento y exploración.

Obtener el acceso es uno de los pasos más importantes en el proceso del ataque, significa el cambio de realizar pruebas en la red (a penetrar en la red), el acceso puede ser a nivel sede sistema, aplicación o de red.

Fase 4: Mantener el acceso. Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos.

En esta fase el intruso intenta permanecer en el sistema, el cual ha comprometido, algunas de las actividades que realiza son agregar usuarios con altos privilegios, robar contraseñas de otros usuarios, o servicios incluso en algunas ocasiones instala herramientas como rootkits, troyanos. Un rootkits es un conjunto de herramientas que le permite al atacante ocultar sus actividades (procesos, sesiones, conexiones) pueden ser a nivel aplicación o incluso a nivel de núcleo.

Fase 5: Borrar huellas. Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro o alarmas del Sistema de Detección de Intrusos (IDs).

Normalmente el atacante elimina la evidencia del ataque y de sus actividades para evitar acciones legales, andar libremente en el sistema comprometido y mantener el acceso.

SOFTWARE ESPÍA (Spyware)

Los programas de espionaje informático envían informaciones del computador del usuario de la red para desconocidos. Hasta lo que es digitado en su teclado puede ser monitoreado por ellos. Algunos tienen un mecanismo que hace una conexión con el servidor del usuario siempre que él estuviera conectado on-line.

La pregunta más frecuente es: ¿Cómo el software de espionaje roba informaciones del PC del usuario?

La respuesta puede ser obtenida cuando el usuario de internet baja algún programa que viene con archivo ejecutable spyware; normalmente el usuario no sabe sobre la amenaza de este archivo y lo instala. Este programa puede obtener informaciones que están en el microcomputador, como las que pasan por él.

Utilizan un método de conexión entre propietario y servidor de forma directa e instantánea. El software de espionaje también puede actuar usando un gerenciador de e-mail para enviar informaciones para una dirección electrónica determinada.

2.2.3. Marco Legal

Los medios virtuales se constituyen en una nueva herramienta de comunicación con el mundo antes desconocido. Posee ventajas y desventajas, una de estas es que existen personas inescrupulosas que valiéndose de conocimientos tecnológicos y/o de sistemas vulneran contraseñas, usuarios, cuentas y demás para cometer delitos informáticos.

Aquí ofrecemos algunas recomendaciones para no ser víctimas de este delito.

Claves programáticas espías: conocidas como troyanos, o software espías, utilizadas para sustraer información en forma remota y física, preferiblemente aquella que le permita al delincuente validarse en el sistema bancario, suplantando a la víctima.

Estafas a través de subastas en línea: se presentan en el servicio de venta de productos, generalmente ilícitos, en línea o en la red; se pueden encontrar celulares hurtados, software de aplicaciones ilegales, además puede ser una vía de estafa ya que se suelen incumplir reglas de envío y de calidad de los productos solicitados.

Divulgación indebida de contenidos: son conductas originadas en el anonimato ofrecido en el internet y el acceso público sin control desde cibercafés; entre ellas se encuentran el envío de correos electrónicos anónimos, con fines injuriosos o calumnias, amenazas y extorsiones.

Pornografía infantil en internet: a través de foros, chats, comunidades virtuales, transferencias de archivos, entre otras modalidades, los delincuentes comercializan material pornográfico que involucra menores de edad.

Violación a los derechos de autor: utilizando reproductores en serie, los delincuentes realizan múltiples copias de obras musicales, video gramas y software.

Piratería en internet: implica la utilización de internet para vender o distribuir programas informáticos protegidos por las leyes de la propiedad intelectual. Aquí encontramos la utilización de tecnología par a par, correo electrónicos; grupos de noticias, chat por replay de internet, orden postal o sitios de subastas, protocolos de transferencia de archivos, etc.

RECOMENDACIONES DE SEGURIDAD CONTRA ESTE DELITO

- Para las claves, use siempre palabras donde mezcle números, letras y símbolos diferentes.
No permita que nadie utilice su usuario, ni conozca sus claves.
- No reenvíe ni abra cadenas de correos, aunque el remitente sea conocido, menos si está en idioma diferente al español.
- Muchos hackers utilizan noticias curiosas o impactantes para lanzar infecciones, troyanos, malware.
- No ingrese a mensajes de correo o links como “Quién te eliminó de Messenger”, es una forma de robar contraseñas.

ORIGEN

La aparición de las nuevas tecnologías origina un doble fenómeno:

- Por un lado, aparecen conductas que, mediante el uso de las nuevas tecnologías de la información, pueden lesionar bienes jurídicos anteriormente protegidos penalmente.
- Por otro, surgen nuevos intereses que demandan protección penal (bienes jurídicos del ciberespacio).

TIPOS DE DELITOS

- Delitos cuyo objeto es causar daños Físicos.
- Delitos cuyo objeto es causar daños Lógicos.
- Ciberdelitos.
- bombas lógicas.

PROPUESTAS DE SOLUCIÓN.

Las principales propuestas de solución planteadas en la investigación son las siguientes:

Creación de nuevas leyes y la reforma del el código penal para tomar en cuantas las sanciones a los delitos informáticos.

La educación eficaz informática a las personas para evitar ser víctima de un delito informático por la ignorancia. Establecer más medidas de seguridad en páginas web destinadas al comercio electrónico

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado “De la Protección de la información y de los datos” que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

DOCUMENTOS DE UNA POLÍTICA DE SEGURIDAD

Un modelo propuesto según la norma ISO 17799 la cual recomienda la aplicación de estándares encaminados a la seguridad informática plantea tres grandes secciones: Las directrices son un conjunto de reglas generales de nivel estratégico donde se expresan los valores de la seguridad de la organización. Es propuesta por el líder empresarial de la organización y tiene como su base la misión y visión para abarcar toda la filosofía de la seguridad de la información.

Las normas son un conjunto de reglas generales y específicas de la seguridad de la información que deben ser usadas por todos los segmentos involucrados en todos los procesos de negocio de la institución, y que deben ser elaboradas por activo, área, tecnología, proceso de negocio, público a que se destina, etc. Las normas de seguridad para usuarios son dirigidas para el uso de ambientes informatizados, basadas en aspectos genéricos como el cuidado con las claves de acceso, manejo de equipos o estaciones de trabajo, inclusión y exclusión de usuarios, administración de sistemas operativos, etc.

Los procedimientos e instrucciones de trabajo son un conjunto de orientaciones para realizar las actividades operativas, que representa las relaciones interpersonales e ínter departamental y sus respectivas etapas de trabajo para su implementación y mantenimiento de la seguridad de la información.

LEY 1273 DE 2009

(Enero 05)

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1º. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: *Obstaculización ilegítima de sistema informático o red de*

telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: *Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

III. MARCO METODOLÓGICO

3.1. TIPO DE INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo ya que se empleara una encuesta como medio de recolección de datos, la cual nos arrojará unos resultados en forma de porcentajes, con el propósito de conocer en realidad si se implementan los mecanismos de seguridad en cualquier empresa.

Por otro lado la investigación tiene un nivel descriptivo, ya que se detalla detenidamente la problemática a nivel mundial y nacional de la seguridad informática, más exactamente en el entorno empresarial en este caso de las empresas de El Carmen de Bolívar como manejan la información y la confidencialidad de los sistemas de información a través de la descripción exacta de las actividades, objetos, procesos y personas.

Se deja constancia del instrumento de investigación pero no se llevara a la práctica. En este caso el diseño de estudio no es experimental.

3.2. POBLACIÓN Y MUESTRA

Se tomara como ya lo mencionamos una de las empresas del sector financiero que será nuestra población, posteriormente se sacara una muestra a la cual se le realizara el respectivo estudio, la muestra de la población serán las personas que trabajan en dichas empresas, que manejen correos electrónicos bases de datos y redes sociales por los cuales intercambian un sin número de información; de esta forma se llevara a cabo la encuesta.

DATOS	Número de Empleados	%
<i>Población</i>	90	100
<i>Muestra</i>	27	30

Población: Empresa con 90 empleados equivale al 100%

Muestra: 27 empleados equivale al 30% de la población.

3.3. OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLES	DIMENSIONES	INDICADORES
V1 Seguridad Informática	Seguridad Protección	Mantener protegida la información confidencial.
V2 Información	Dato Conocimiento	Representar simbólicamente una característica personal o de una entidad
V3 IDs	Control Revisión	Detectar manipulaciones no deseadas en el sistema, especialmente a través de internet.
V4 Ataque Informático	Debilidad Robo	Aprovechar vulnerabilidades en el sistema a fin de obtener un beneficio propio
V5 Ciberespacio	Redes Internet información	Espacio virtual donde se agrupan usuarios, páginas web, chats, (redes sociales) y demás servicios de Internet.

3.4. INSTRUMENTOS Y TECNICAS DE INVESTIGACION

Los instrumentos fueron creados en la herramienta formularios de GOOGLE DRIVE.

ANEXO: Los link de los instrumentos para mayor visualización,

CUESTIONARIO EN PRO DE LA SEGURIDAS INFORMATICA

<https://docs.google.com/forms/d/1ENu7HkwCzkO41n2wtS3QrOGKoY0M0q44YrJ2IP9cKJg/viewform>

ENCUESTA DE SATISFACCIÓN EN PRO DE LA SEGURIDAD INFORMATICA

https://docs.google.com/forms/d/1tpTm_EAmMkNtdmWYcjax0NJL-May9Gj7IN5koTwFJkk/viewform

Cuestionario en Pro de la Seguridad Informatica

Preguntas para saber el nivel de seguridad al compartir información

¿Utiliza redes sociales en tiempos laborales?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO
- ☐ NO ES PERMITIDOS ESTÁN BLOQUEADAS

¿Considera que usted aporta a la seguridad de su empresa?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO
- ☐ ALGUNAS VECES

¿Dedica tiempo para ver o llenar publicidades en Internet en horas laborales?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO

¿Comparte información confidencial con compañeros de trabajo mediante medios que no sean propios de la empresa?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO
- ☐ ALGUNAS VECES

¿Le ha facilitado contraseñas a compañeros no autorizados por la empresa?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO

¿Considera que el antivirus que maneja la empresa es suficientemente seguro y confiable?

Marque solo una de las siguientes

- ☐ POCO SEGURO
- ☐ SEGURO
- ☐ MUY SEGURO

¿Reconoce las modalidades de delitos informáticos?

Marque solo una de las siguientes preguntas

- ☐ SI
- ☐ NO

¿tiene precaución a la hora de descargar e instalar programas en su computador asignado en la empresa?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO

¿Revisa o reenvía cadenas de correos con publicidad así sean de remitentes conocidos?

Marque solo una de las siguientes opciones

- ☐ SI
- ☐ NO

¿Que medidas de seguridad toma para evitar ser víctima de delincuentes informáticos?

Puede marcar mas de una opcion

- ☐ Hago uso de un buen antivirus en mi computador
- ☐ No doy contraseñas a conocidos
- ☐ Mantengo copia de seguridad de información confidencial
- ☐ No doy información personal por redes sociales
- ☐ Ninguna de las anteriores

Enviar



Encuesta de Satisfacción en Pro de la Seguridad Informatica

Son tres preguntas en las cuales conoceremos su aponion acerca del nivel de seguridad de su empresa y su satisfaccion con el mismo

Como considera que esta el modelo de seguridad en la empresa

Marque solo una de las siguientes opciones

- ☐ INSUFICIENTE
- ☐ ACEPTABLE
- ☐ SOBRESALIENTE
- ☐ EXCELENTE

En qué grado considera que esta preparado para enfrentar las amenazas informáticas externas que afecten a su organización

Marque solo una de las siguientes opciones

- ☐ INSUFICIENTE
- ☐ ACEPTABLE
- ☐ SOBRESALIENTE
- ☐ EXCELENTE

Como cree usted que son los mecanismos de autenticación y validación de datos de su empresa.

Marque solo una de las siguientes opciones

- ☐ INSUFICIENTES
- ☐ ACEPTABLES
- ☐ SOBRESALIENTES
- ☐ ECXELENTES

Se siente satisfecho con los mecanismos o grado de protección de su información

Marque solo una de las siguientes opciones

- ☐ INSATISFECHO
- ☐ POCO SATISFECHO
- ☐ SATISFECHO
- ☐ MUY SATISFECHO

Enviar

3.5. RESULTADOS ESPERADOS

El principal objetivo que se espera de la encuesta que deseamos efectuar a los empleados, es reconocer si se da un buen uso de manejo de información o si por el contrario, los empleados no toman las precauciones necesarias para intercambiar datos.

Se efectuaran unas preguntas que nos ayude a saber qué es lo que pasa en realidad.

Por otro lado Se realizará un cuestionario esperando establecer que tan segura es la confidencialidad de la información en dicha empresa y mediante qué mecanismos de control en redes maneja para evitar delitos informáticos

4. BIBLIOGRAFÍA

Información

www.segu-info.com

<http://www.segu-info.com.ar/tesis/>

www.slideshare.net

<http://www.slideshare.net/MOSHERG/tesis-plan-de-seguridad-informatica>

www.ilustrados.com

<http://www.ilustrados.com/documentos/jp-Protocolo%20delitos%20informaticos.pdf>

www.policia.gov.co

www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Servicios_Especializados/area_infancia_adolescencia/red_educadores/herramientas/012_DELITOS_INFORMATICO.pdf

<http://tesis.ipn.mx/dspace/bitstream/123456789/498/1/TESIS%20PROPUESTA%20SEGURIDAD.pdf>

Legal

www.policia.gov.co

http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

www.deltaasesores.com

<http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia>

BS7799:1 “Information Security Management- Part 1: Code of practice for information security management” - **Ciro Antonio Dussán Clavijo** Administrador informático.

www.beorlegui.files.wordpress.com

<http://beorlegui.files.wordpress.com/2011/10/delitos-informaticos-y-ciberterrorismo.pdf>

www.alcaldiabogota.gov.co

<http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492>